



Polska wersja tego dokumentu znajduje się [tutaj](#):

Certificate Policy Telekomunikacja Polska Secure Corporate Mail

Table of contents

1.	Introduction.....	3
1.1	Document identification	3
1.2	Change history	3
1.3	Service recipients and applicability of the certificates	4
1.4	Contact data	4
2.	Basic principles of certification	4
2.1	Issued certificates	4
2.2	Rights and obligations	5
2.3	Responsibilities of the Signet Certification Center.....	6
2.4	Fees	7
2.5	Publishing the issued certificates and revocation information	7
2.6	Information protection.....	7
2.7	Interpretation and the applicable law.....	7
2.8	Intellectual property rights	7
3.	Identity verification and authentication	7
3.1	Registration	7
3.2	Issuing the test certificates	9
3.3	Superseding the keys.....	9
3.4	Suspending a certificate	9
3.5	Reinstating a certificate	10
3.6	Revoking a certificate	10
3.7	Renewing a certificate	10
4.	Operational requirements	10
4.1	Submitting a certificate request.....	10
4.2	Issuing a certificate	10
4.3	Accepting a certificate	11
4.4	Suspending a certificate	11
4.5	Reinstating a certificate	11
4.6	Revoking a certificate	11
4.7	Renewing a certificate	11
4.8	Recovering the private key.....	12
5.	Technical security measures	12
5.1	Key generation	12
5.2	Protection of the keys.....	12
5.3	Activating the keys	12
5.4	Destroying the keys.....	12
6.	Adjustment of the Policy provisions to the user requirements	13
7.	Certificate profile and Certificate Revocation Lists (CRL).....	13
7.1	Signature/encryption certificate profile	13
7.2	Mobile-device certificate profile	16
7.3	Server certificate profile.....	17
7.4	VPN certificate profile.....	21
7.5	Domain-controller certificate profile	22
7.6	Software certificate profile	23
7.7	Test certificate profiles	25
7.8	Certificate Revocation List (CRL) profile	25

1. Introduction

This Certificate Policy (“Policy”) defines, in technical and organizational terms, the methods, scope, and conditions for the protection, creation, and use of certificates to secure the electronic mail and devices used by the TP Group companies.

The certification services described herein are provided by the Signet Certification Center (“Signet CC”) operated by Telekomunikacja Polska S.A. with its registered office address of 00-105 Warszawa, ul. Twarda 18 (“TP”).

1.1 Document identification

Title	Certificate Policy — Telekomunikacja Polska Secure Corporate Mail
Reservation	Certificate issued in compliance with the “Certificate Policy — Telekomunikacja Polska Secure Corporate Mail” document
Version	1.7
OID (Object Identifier)	1.3.6.1.4.1.27154.1.1.20.10.1.1.7
Implementing entity	TELEKOMUNIKACJA POLSKA CA
Issue date	10.06.2010
Expiration date	Until revoked
Certification Practice Statement	KPC Centrum Certyfikacji Signet (CPS CC Signet) 1.3.6.1.4.1.27154.1.1.1.1.1.0

1.2 Change history

Version	Date	Change description
1.0	15.12.2006	The first version of the document.
1.1	22.01.2007	Adding certificates for mobile devices. Adding details to the principles of issuing test certificates, extending their maximal validity period to 60 days.
1.2	25.09.2007	Defining the Subject field for certificates of TP Group employees, adding the possibility to issue VPN certificates for IP addresses of TP business partners.
1.3	07.12.2007	Changing the address of the website with information on the service, Certificate Policy, and CRL. Removing the CDP ldap points. Adding the possibility to suspend certificates by Signet CC for technical reasons.
1.4	25.07.2008	Changing the address of the website with information on the service, Certificate Policy, and CRL (returning to the address www.bptp.lodz.telekomunikacja.pl , now accessible also from the Internet). Changes in the procedures for requesting, revoking, suspending, and reinstating certificates, resulting from deploying the certificate management module for TP employees, integrated with the identity management system (ITIM). Removing the references to outsourcing the service to an external provider.
1.5	17.10.2008	Adding the optional attributes dNSName and iPAddress in the subjectAltName extension to the server certificate. Extending the maximal CRL validity period to 72 hours.
1.6	26.02.2009	Adding an alternative profile to the server certificate for an SSL client.
1.7	10.06.2010	Updating the certificate renewal and issuance process. Changing the content of the subject field in the signature and encryption certificates for non-TP employees. Adding the optional extension extendedKeyUsage to the VPN certificate profile. Adding a certificate profile for a server acting as both an SSL client and server. Other minor editorial corrections.
1.7	24.02.2011	Changes in mobile device certificate profile: limitation of certificate validity period to 1 year, adding an optional attribute OU in Subject field, correction of mistyped text in policyQualifierID extension.

Unless stated otherwise, any change is applicable to the certificates issued after the date of the given version of the Policy. Each certificate issued by Signet CC contains a reference to the full text of the Policy applicable for such certificate.

1.3 Service recipients and applicability of the certificates

The certificates issued hereunder are applicable to natural persons employed by TP and to devices used or administered by such persons.

The recipients of the certification services hereunder are persons employed by TP, classified into the following categories:

- LRAO (Local Registration Authority Officer) — a representative of the TP Certification Authority (TP CA)
- TPA (TP administrator) — the administrator the end users communicate with
- Administrator — a person employed by TP, responsible for the operation of a device secured with a certificate issued hereunder
- End users

The following types of certificates are issued hereunder:

- certificate for digital-signature verification and authentication (“signature certificate”)
- certificate for encrypting e-mail messages (“encryption certificate”)
- certificate for encrypting e-mail messages for function email-accounts shared by a group of authorized End Users (“function encryption certificate”)
- certificate for authorization of mobile devices in wireless networks [(“mobile device certificate”)]
- certificate to secure servers with the SSL protocol (“server certificate”)
- certificate for establishing connections in virtual private networks (“VPN certificate”)
- certificate for authorizing domain-controller servers (“domain-controller certificate”)
- certificate for signing the software distributed within the TP Group (“software certificate”) — it enables detecting any changes in the software code, introduced after signing it, and guarantees the code authenticity (i.e. that it has been signed by the issuer identified by the certificate).

1.4 Contact data

For more information on the Signet CC services provided hereunder, please contact:

Telekomunikacja Polska S.A.
Centrum Certyfikacji Signet
ul. Czackiego 13/15
00-043 Warszawa
E-mail: BP.TP@telekomunikacja.pl

2. Basic principles of certification

2.1 Issued certificates

Signet CC issues hereunder the following certificates:

- signature certificates

- encryption certificates
- mobile device certificates
- server certificates
- VPN certificates
- domain-controller certificates
- software certificates.

The signature certificates issued hereunder are not qualified certificates for the purposes of the Digital Signature Act of 18.09.2001 (Journal of Laws 130.1450). A digital signature verified through such certificate does not have the legal effects equivalent to a handwritten signature, unless the user agrees in writing to such treatment of such digital signature.

The encryption certificates are not used to verify a digital signature.

The mobile-device certificates and software certificate issued hereunder are not qualified certificates for the purposes of the Digital Signature Act of 18.09.2001 (Journal of Laws 130.1450). A digital signature verified through such certificate does not have the legal effects equivalent to a handwritten signature.

The server certificates, VPN certificates, and domain-controller certificates issued hereunder are not certificates for the purposes of the Digital Signature Act of 18.09.2001, because they assign a public key to a device.

The table below defines the holders of various types of certificates, i.e. the persons identified by the certificate or the persons responsible for the operation of a device identified by the certificate:

Certificate	Certificate holder
signature certificate	LRAO, TPA, Signet CC operator, or End User
encryption certificate	LRAO, TPA, or End User
function encryption certificate	LRAO, TPA, or End User
mobile device certificate	End User
server certificate	Administrator
VPN certificate	Administrator
domain-controller certificate	Administrator
software certificate	End User

2.2 Rights and obligations

2.2.1 Obligations of the certificate holder

Prior to requesting the certificate, the requester must get acquainted with this Policy. Submitting a request is equivalent to acceptance of the terms and conditions of the certificate issuance service hereunder. The requester is responsible for trueness of the data provided in the certificate request.

The certificate holder must securely store the private key associated to the public key contained in his/her certificate.

If the certificate holder loses control of such private key or if the private key is revealed (or believed to be revealed), he/she must notify the certificate issuer without delay by submitting the certificate revocation request. The certificate holder is responsible for trueness of the data provided in the certificate request.

If the keys are generated independently by the Administrator, the Administrator is responsible for the quality of the generated key pair containing the public key provided in the certificate request.

The certificate holder must notify the certificate issuer of any changes of the information provided in the certificate or in the certificate request.

Upon receipt of the certificate, the certificate holder must verify the certificate contents.

Upon expiration or revocation of the certificate, the certificate holder must cease to use the private key associated with the public key contained in the certificate, except if the certificate is renewed without changing the keys.

2.2.2 Obligations of the trusting party

The trusting party must securely download the certificate of the trusted CA (Certification Authority) and verify its public key. The methods of getting access to the CA certificates and to the information necessary to verify them are described in the Certification Practice Statement.

As part of establishing the trust in a service based on a certificate issued hereunder, the trusting party must properly verify the certificate. Within the verification process, the trusting party must verify the whole certification path. A certification path is an ordered sequence including CA certificates and the verified certificate, created so that each next certificate in the path can be verified as based on the previous certificate in the path, assuming the first certificate in the path as the trustworthy starting point.

In the verification process, the trusting party should use the resources and procedures provided by Signet CC.

The Certification Practice Statement defines the available services and methods of verification of the certificate validity. The trusting party is obliged at least to use the Certificate Revocation List ("CRL") published by Signet CC and to verify the certification path from the trusted CA to the certificate issuer.

2.2.3 Obligations of the Signet Certification Center

The certification services are provided by Signet CC in compliance with the legal regulations in force in Poland. Signet CC is obliged to comply with this Policy and in particular to execute the certificate registration, renewal, and revocation procedures in compliance herewith.

Signet CC must ensure that each private key associated with the public key contained in any encryption certificate issued hereunder is stored for at least 5 years from the moment of its archiving (which must take place immediately after generating the certificate).

2.3 Responsibilities of the Signet Certification Center

Signet CC is responsible for consistency of the information contained in the certificate with the information provided in the certificate request.

Signet CC is not responsible for trueness of the information provided in the certificate request. The scope and method of verification of the information provided in the certificate request are described in Section 3 below.

Signet CC is responsible for compliance with the adopted procedures and in particular for publishing up-to-date information on certificate revocation in the Signet CC Repository in compliance herewith.

2.4 Fees

The certificate issuance and renewal services hereunder are free of charge.

The certificate revocation services and the revocation information (CRL) are free of charge.

2.5 Publishing the issued certificates and revocation information

Signet CC publishes the certificate revocation lists in the publicly available Repository at <http://www.btp.lodz.telekomunikacja.pl/repozytorium/>.

The signature certificates and encryption certificates are published in the TP corporate catalog services immediately after their issuance.

The certificate revocation information is published at the moment of generation of a new CRL. A new CRL hereunder must be generated without delay after each revocation, but not less frequently than every 72 hours.

2.6 Information protection

The information collected and processed hereunder is protected in compliance with the legal regulations. Signet CC guarantees that the only information made available outside the TP corporate network are the publicly available CRLs. Users of the TP corporate network additionally have access to the information contained in the issued certificates.

The above restrictions do not apply to revealing information to competent Polish authorities in compliance with the law.

2.7 Interpretation and the applicable law

To the extent of the certificates issued hereunder, Signet CC operates in compliance with the Signet CC Certification Practice Statement and with this Policy. In case of doubt, the provisions of those documents shall be interpreted in compliance with the superior legal regulations in force in Poland.

2.8 Intellectual property rights

The proprietary rights to this Policy belong exclusively to Telekomunikacja Polska S.A.

3. Identity verification and authentication

This section describes the procedure of verification of identity of a person performing a certificate-management operation and the procedure of verification of such person's authorization to perform the given activity.

3.1 Registration

The registration process, i.e. the process of accepting and verifying a new certificate request, is performed by the Signet CC Registration Authority, a department of TP CA. If the registration process is completed positively, TP CA issues the requested certificate.

The detailed registration steps for various certificate types are described in the operational procedures. A general description of the registration process is provided in Section 4 below.

The requester must provide the following data for the registration process:

1. For signature certificates, encryption certificates, and function encryption certificates:
 - a. full name of the requested certificate holder
 - b. identification No. of the requested certificate holder (applicable to TP employees)
 - c. name of the organizational unit employing the requested certificate holder
 - d. e-mail address (compliant with the SMTP standard) of the certificate holder
 - e. business address to which a data medium with the issued certificates and related keys is to be sent.

NOTE: In case of a function encryption certificate, one issued certificate is used by all users of the given e-mail account.

2. For mobile device certificates:
 - a. the IMEI number (to be placed in the UPN attribute of the **subjectAltName** extension)
 - b. e-mail address (compliant with the SMTP standard) of the mobile device owner
 - c. full name of the mobile device owner.
3. For VPN certificates and server certificates:
 - a. address of the server for which the certificate is requested
 - b. name of the organizational unit in which the server is installed
 - c. e-mail address (compliant with the SMTP standard) of the Administrator responsible for the server
 - d. the public key to be included in the certificate.
4. For domain controller certificates:
 - a. The DN value (to be placed in the **subject** field)
 - b. the GUID value (to be placed in the **otherName** attribute of the **subjectAltName** extension)
 - c. domain name of the domain controller (to be placed in the **dnsName** attribute of the **subjectAltName** extension)
 - d. e-mail address (compliant with the SMTP standard) of the Administrator responsible for the domain controller (to be placed in the **rfc822Name** attribute of the **subjectAltName** extension).
5. For software certificates:
 - a. full name of the certificate holder (if it is to be included in the certificate)
 - b. The CN value (to be placed in the **subject** field)
 - c. e-mail address (compliant with the SMTP standard) of the person responsible for using the certificate (to be placed in the **rfc822Name** attribute of the **subjectAltName** extension)
 - d. the public key to be included in the certificate (only if the key pair is generated by the requested certificate holder).

The process of registration of a signature certificate or encryption certificate includes verification of the identity of the requester and of the requested certificate holder, as well as verification of their employment by TP, against respective TP databases.

The process of registration of a VPN certificate or server certificate includes verification of the following:

- correctness of the server address:
 - in case of a certificate for a domain address:
 - whether the domain name indicated in the request is assigned to TP (as confirmed by the relevant name-space managing authority), or
 - whether the domain name indicated in the request does not belong to the Internet name space (does not end with any top-level domain name)
 - in case of a certificate for an IP address:
 - whether the indicated address belongs to the private address class, or
 - whether the address belongs to a class assigned to TP (or — if the certificate is requested by a TP business partner — to such TP business partner), as confirmed by Réseaux IP Européens (www.ripe.net) or an equivalent authority relevant for the given IP address range (or as declared by the business partner)
- possession of a private key associated with the key included in the request (the request must comply with the PKCS#10 standard).

The process of registration of a domain-controller certificate includes verification of the requester's authorization to submit the request, in compliance with the operational procedures.

The process of registration of a software certificate includes verification of the requester's authorization to submit the request, in compliance with the operational procedures.

3.2 Issuing the test certificates

It is allowed to issue hereunder test certificates of all types envisaged herein. The validity period of a test certificate may not exceed 60 days. Test certificates may not be requested by End Users.

Test certificates may be requested by the persons envisaged in the operational procedures contemplated above, as well as by managers of TP Projects in which the certificates are to be used. The process of registration of a test certificate includes verification of the requester's authorization to submit the request. The data to be included in the test certificate is not verified and the requester is responsible for its correctness.

3.3 Superseding the keys

No procedure is available for key superseding, i.e. for issuing a new certificate with a new public key during the validity period of an existing certificate, under a simplified registration process.

The keys can be superseded only through submitting a new certificate request with a new public key, as described in section 4.1 below.

3.4 Suspending a certificate

A certificate issued hereunder may be suspended by the user through the ITIM system or by an authorized TPA or LRAO through the relevant website.

Also, a certificate may be suspended by Signet CC in the cases contemplated in section 4.6 below or due to technical reasons.

Furthermore, a certificate may be suspended automatically upon receipt of a notification from the TP human-resource department that the certificate holder's employment has been terminated.

3.5 Reinstating a certificate

A suspended certificate may be reinstated by the user through the ITIM system or by an authorized TPA or LRAO through the relevant website.

Also, Signet CC shall reinstate a suspended certificate if the cause of suspension ceases to exist.

3.6 Revoking a certificate

Revoking a certificate issued hereunder requires submitting a certificate revocation request, which is subject to authentication of the requester and verification of the requester's authorization to submit such request.

A certificate for a TP employee may be also revoked through the certificate management module integrated with the ITIM system (subject to authentication) or through the Service Desk (subject to authentication of the certificate holder), effectively by the LRAO.

Furthermore, the LRAO may revoke a certificate on request of the certificate holder's superior.

3.7 Renewing a certificate

A certificate issued hereunder may be renewed. The renewal consists in issuing a new certificate with the same personal data as in the old certificate.

A certificate may be renewed only within the validity period of the old certificate and only if the data the certificate is based upon remains unchanged. After the validity period or if the data is changed, the certificate holder must apply for a new certificate under the registration procedure contemplated in section 3.1 above.

The certificate renewal process includes verification of the requester's identity using the cryptographic method, against the private key associated with the public key contained in the renewed certificate.

4. Operational requirements

4.1 Submitting a certificate request

As conditions for issuing a certificate hereunder, the future certificate holder must get acquainted with the service terms and conditions and must submit a valid certificate request.

4.2 Issuing a certificate

The certificate shall be issued within 5 (five) workdays of receipt by Signet CC of a valid certificate request.

4.3 Accepting a certificate

Upon issuing the certificate, the holder must verify whether the certificate data is consistent with the certificate request. If any discrepancy is detected, the certificate holder must notify Signet CC without delay, submit a request to revoke the defective certificate, and not use the private key associated with the public key contained in the certificate. In absence of any objections within 24 hours, the certificate shall be deemed verified against the data provided in the certificate request.

If the data included in the certificate is inconsistent with the certificate request, Signet CC shall issue a new certificate with the correct data.

If the certificate holder accepts a certificate with data inconsistent with the certificate request, he/she shall be responsible for any consequences of using such certificate, attributable to such inconsistency.

4.4 Suspending a certificate

A certificate may be suspended on request of the certificate holder or his/her superior or through a decision of Signet CC in compliance with its internal procedures.

4.5 Reinstating a certificate

A suspended certificate may be reinstated on request of an authorized person or through a decision of Signet CC in compliance with its internal procedures.

4.6 Revoking a certificate

A certificate issued hereunder may be revoked.

The requester must be authenticated as described in section 3.6 above. If the requester's authorization to submit the certificate revocation request is verified positively, the certificate becomes revoked irreversibly. To revoke a certificate, the requester must:

- submit a certificate revocation request to the identity management system, or
- contact the TP Group Service Desk, provide all information necessary to unequivocally identify the requester and the certificate, and request the certificate to be revoked.

Furthermore, Signet CC may revoke a certificate in the following cases:

- upon receipt of a written revocation request from the certificate holder or an authorized third party
- if the information included in the certificate becomes out-of-date
- if the certificate has been issued illegally or incorrectly, such as due to:
 - non-compliance with essential preconditions for issuing the certificate
 - providing false data for the certificate
 - errors in data entry or in the processing.

In case of a justified suspicion that the certificate should be revoked, Signet CC shall suspend the certificate, notify the certificate holder, and investigate the situation.

4.7 Renewing a certificate

A certificate issued hereunder may be renewed, but only during the period of validity of the old certificate. After the validity period, the certificate holder must apply for a new certificate under the registration procedure contemplated in section 4.1 above.

4.8 Recovering the private key

Copies of the private keys associated with encryption certificates are stored in Signet CC and can be recovered.

5. Technical security measures

5.1 Key generation

Any key pair out of which the public key is certified hereunder must be based on the RSA algorithm and comply with the following requirements:

Certificate type	Minimal key length (modulus of $p \cdot q$)	Key generation method	Key generating entity
signature certificate	1024 bits	on a chip card	Signet CC
encryption certificate, function encryption certificate	1024 bits	in a secure environment	Signet CC
mobile device certificate	1024 bits	no requirements	Signet CC or certificate holder
server certificate	1024 bits	no requirements	Certificate holder
VPN certificate	1024 bits	no requirements	Certificate holder
domain-controller certificate	1024 bits	in a secure environment	Signet CC
software certificate	1024 bits	no requirements	Signet CC or certificate holder

5.2 Protection of the keys

The certificate holder is solely responsible for protecting the private key from the moment of its generation (in case of a server certificate or VPN certificate) or from the moment of its receipt (in case of a signature certificate, encryption certificate, mobile-device certificate, or domain-controller certificate).

In case of a software certificate, the certificate holder is solely responsible for protecting the private key from the moment of its generation (if the key pair is generated by the holder) or from the moment of its receipt (if the key pair is generated by Signet CC).

In case of a function encryption certificate and Signet CC operator certificate, responsibility for protection of the private key rests with each person authorized to use the certificate.

Signet CC is responsible for protecting the copy of a private key associated with an encryption key, stored in Signet CC, until such copy is destroyed.

5.3 Activating the keys

This Policy imposes no requirements on the method of activation of the private key by the certificate holder.

5.4 Destroying the keys

This Policy imposes no particular requirements on the method of destroying a private key associated with a public key included in a certificate issued hereunder.

Upon expiration of a signature certificate issued hereunder, the private key associated with the public key included in such certificate should be deleted from the card (using the software provided by Signet CC) or access to such key should be disabled irrevocably, except if the certificate is renewed without changing the keys.

In case of a server certificate, VPN certificate, or domain-controller certificate, the public key associated with such certificate should be deleted from the device in compliance with the instructions for the standard device-management software.

In case of a software certificate, the associated private key should be deleted from its medium or access to such key should be disabled irrevocably.

The private key associated with an encryption certificate issued hereunder may be used to decrypt the data, but must be stored in a secure manner.

Signet CC shall destroy the private key copy stored in the secure archive after 5 years of its archiving.

6. Adjustment of the Policy provisions to the user requirements

A given version of this Policy may not be adjusted in any way to the user requirements. On a justified request of TP Project Managers, a new version of this Policy may be developed to address the proposed requirements.

7. Certificate profile and Certificate Revocation Lists (CRL)

This section describes the certificate profiles and the Certificate Revocation Lists (CRL) for certificates issued hereunder.

For the basic fields of the certificate and CRL, the “Attribute” column provides the field/attribute name as per the standard X.509 v. 3.

The attribute values for the **Issuer** and **Subject** fields are provided in the order from the catalog tree root, as per the standard X.500.

For the certificate and CRL extensions, the “Extension” column provides the extension/attribute name and the respective object identifier. The “Critical extension?” column identifies whether the given extension is critical.

The “Value” column provides the field/attribute value or, after the ‘#’ character, a description of the method of determining the field value and comments.

7.1 Signature/encryption certificate profile

The certificates issued hereunder have the following structure:

Attribute	Value
Version	2 # certificate compliant with X.509 v. 3
serialNumber	# a number assigned by TP CA, unique within the authority
signature	1.2.840.113549.1.1.5 #SHA1 with RSA encryption (identifier of the algorithm used for electronic confirmation of the certificate)
issuer	C = PL, O = Grupa TELEKOMUNIKACJA POLSKA, OU = Centrum Certyfikacji Signet, OU = CA TELEKOMUNIKACJA POLSKA # specific name of the CA issuing the

	certificates hereunder
validity	# certificate validity period
not before	# certificate issuance date and time (GMT in the UTCTime format)
not after	# certificate issuance date + 1,096 days (GMT in the UTCTime format)
subject	C = PL, O = Grupa TELEKOMUNIKACJA POLSKA, OU = # as described below CN = # as described below Title = # name of the certificate holder's position (optional attribute) E-mail = # as described below
subjectPublicKeyInfo	
algorithm	rsaEncryption # identifier of the algorithm associated with the certificate holder's public key
subjectPublicKey	# certificate holder's public key

The value of the CN attribute in the **subject** field is as follows:

- function name (for a function encryption certificate)
- <surname> <given name(s)> / **Nr Ew.** <id No.> # (for TP Group employees)
- <surname> <given name(s)> - **Partner TP DSN:** <serial No. of the issued medium> # (in other cases) (not applicable to a renewed certificate, in which the CN value is identical as in the old certificate)

The value of the OU attribute in the **subject** field is as follows:

- in case of a TP Group employee: "<company name>"
- in case of other employees: "<company name> - **Partner TP**"

The value of the E-mail attribute in the **subject** field is as follows:

- function e-mail box address (for a function encryption certificate)
- certificate holder's e-mail address (in other cases).

NOTE: No diacritical marks are allowed in the **subject** field.

The certificate contains the following extensions compliant with X.509:

Extension	Critical extension?	Value
keyUsage 2.5.29.15	YES	# as described below
(0) digitalSignature	-	# digital signature key 1 # for a signature certificate 0 # for an encryption certificate
(1) nonRepudiation	-	0
(2) keyEncipherment	-	# key-exchange key 0 # for a signature certificate 1 # for an encryption certificate
(3) dataEncipherment	-	# data encryption key 0 # for a signature certificate 1 # for an encryption certificate
(4) keyAgreement	-	0
(5) keyCertSign	-	0
(6) crlSign	-	0
(7) encipherOnly	-	0
(8) decipherOnly	-	0
extendedKeyUsage 2.5.29.37	NO	# as described below
authorityKeyIdentifier 2.5.29.35	NO	-

keyIdentifier	-	# identifier of the CA key, for verification of the certificate signature
subjectKeyIdentifier 2.5.29.14	NO	# identifier of the certificate holder's key identified in the subjectPublicKeyInfo field
basicConstraints 2.5.29.19	NO	-
cA	-	FALSE
subjectAltName 2.5.29.17	NO	# alternative name of the certificate holder
rfc822Name	-	# as described below
UPN	-	# user_domain_name@domain_name — applicable only to signature certificates
cRLDistributionPoint 2.5.29.31	NO	-
distributionPoint	-	http://www.bptp.lodz.telekomunikacja.pl/repozytorium/crl/catp.crl
certificatePolicies 2.5.29.32	NO	-
policyIdentifier	-	1.3.6.1.4.1.27154.1.1.20.10.1.1.7
policyQualifierID 1.3.6.1.5.5.7.2.1	-	http://www.bptp.lodz.telekomunikacja.pl/repozytorium/docs/pc_bptp_1_7.pdf
qualifier 1.3.6.1.5.5.7.2.2	-	# as described below

The value in the **keyUsage** field is as follows:

- for a signature certificate: 80h [hex]
- for an encryption certificate: 30h

The value in the **extendedKeyUsage** field is as follows:

- for a signature certificate:
 1.3.6.1.5.5.7.3.2 (id-kp-clientAuth),
 1.3.6.1.5.5.7.3.4 (id-kp-emailProtection),
 1.3.6.1.4.1.311.20.2.2 (smartCardLogon);
- for an encryption certificate:
 1.3.6.1.5.5.7.3.4 (id-kp-emailProtection).

The value of the **rfc822Name** field of the **subjectAltName** extension is as follows:

- function e-mail box address (for a function encryption certificate)
- certificate holder's e-mail address (in other cases).

The value in the **CertificatePolicies/qualifier** field is as follows:

- for a signature certificate:

Certyfikat wystawiony zgodnie z dok. "Polityka Certyfikacji - Bezpieczna Poczta Korporacyjna Telekomunikacja Polska". Nie jest certyfikatem kwalifikowanym w rozumieniu ustawy o podpisie elektronicznym (Certificate issued in compliance with the "Certificate Policy — Telekomunikacja Polska Secure Corporate Mail" document. Not a qualified certificate as defined by the Digital Signature Act)

- for an encryption certificate:

Certyfikat wystawiony zgodnie z dokumentem "Polityka Certyfikacji - Bezpieczna Poczta Korporacyjna Telekomunikacja Polska". Nie jest certyfikatem do weryfikacji podpisu elektronicznego. (Certificate issued in compliance with the "Certificate Policy

— Telekomunikacja Polska Secure Corporate Mail” document. Not a certificate for verification of a digital signature.)

7.2 Mobile-device certificate profile

A mobile-device certificate has the following structure:

Attribute	Value
Version	2 # certificate compliant with X.509 v. 3
serialNumber	# a number assigned by TP CA (Signet CC), unique within the authority
signature	1.2.840.113549.1.1.5 #SHA1 with RSA encryption (identifier of the algorithm used for electronic confirmation of the certificate)
issuer	C = PL, O = Grupa TELEKOMUNIKACJA POLSKA OU = Centrum Certyfikacji Signet, OU = CA TELEKOMUNIKACJA POLSKA # specific name of the CA issuing the certificates hereunder
validity	# certificate validity period
not before	# certificate issuance date and time (GMT in the UTCTime format)
not after	# certificate issuance date and time + 1 year (GMT in the UTCTime format)
subject	C = PL O = Grupa TELEKOMUNIKACJA POLSKA OU = Mobile OU= #optional attribute identifying certificates issued in OU = Mobile CN = device name or IMEI number
subjectPublicKeyInfo	
algorithm	rsaEncryption # identifier of the algorithm associated with the certificate holder’s public key
subjectPublicKey	# certificate holder’s public key

The certificate contains the following extensions compliant with X.509:

Extension	Critical extension ?	Value
keyUsage 2.5.29.15	YES	80h
(0) digitalSignature	-	1 # digital signature key
(1) nonRepudiation	-	0
(2) keyEncipherment	-	0
(3) dataEncipherment	-	0
(4) keyAgreement	-	0
(5) keyCertSign	-	0
(6) crlSign	-	0
(7) encipherOnly	-	0
(8) decipherOnly	-	0
extendedKeyUsage 2.5.29.37	NO	1.3.6.1.5.5.7.3.2 #id-kp-clientAuth
authorityKeyIdentifier 2.5.29.35	NO	-
keyIdentifier	-	# identifier of the CA key, for verification of the certificate signature
subjectKeyIdentifier 2.5.29.14	NO	# identifier of the certificate holder’s key identified in the subjectPublicKeyInfo field
basicConstraints 2.5.29.19	NO	-
cA	-	FALSE
subjectAltName 2.5.29.17	NO	
UPN	-	# IMEI_number or name@domain

cRLDistributionPoint 2.5.29.31	NO	-
distributionPoint	-	http://www.bptp.lodz.telekomunikacja.pl/repozytorium/crl/catp.crl
certificatePolicies 2.5.29.32	NO	-
policyIdentifier	-	1.3.6.1.4.1.27154.1.1.20.10.1.1.7
policyQualifierID 1.3.6.1.5.5.7.2.1	-	http://www.bptp.lodz.telekomunikacja.pl/repozytorium/docs/pc_bptp_1_7.pdf
qualifier 1.3.6.1.5.5.7.2.2	-	Certyfikat wystawiony zgodnie z dok. "Polityka Certyfikacji - Bezpieczna Poczta Korporacyjna Telekomunikacja Polska". Nie jest certyfikatem kwalifikowanym w rozumieniu ustawy o podpisie elektronicznym # (Certificate issued in compliance with the "Certificate Policy — Telekomunikacja Polska Secure Corporate Mail" document. Not a qualified certificate as defined by the Digital Signature Act)

7.3 Server certificate profile

A server certificate has the following structure:

Attribute	Value
version	2 # certificate compliant with X.509 v. 3
serialNumber	# a number assigned by TP CA, unique within the authority
signature	1.2.840.113549.1.1.5 #SHA1 with RSA encryption (identifier of the algorithm used for electronic confirmation of the certificate)
issuer	C = PL, O = Grupa TELEKOMUNIKACJA POLSKA OU = Centrum Certyfikacji Signet, OU = CA TELEKOMUNIKACJA POLSKA # specific name of the CA issuing the certificates hereunder
validity	# certificate validity period
not before	# certificate issuance date and time (GMT in the UTCTime format)
not after	# certificate issuance date and time + 1,096 days (GMT in the UTCTime format)
subject	C = PL O = Grupa TELEKOMUNIKACJA POLSKA OU = TELEKOMUNIKACJA POLSKA OU = SSL CN = # server IP address or domain name
subjectPublicKeyInfo	
algorithm	rsaEncryption # identifier of the algorithm associated with the certificate holder's public key
subjectPublicKey	# certificate holder's public key

The certificate contains the following extensions compliant with X.509:

Extension	Critical extension?	Value
keyUsage 2.5.29.15	YES	80h
(0) digitalSignature	-	1 # digital signature key
(1) nonRepudiation	-	0
(2) keyEncipherment	-	1 # key-exchange key
(3) dataEncipherment	-	1 # data encryption key
(4) keyAgreement	-	0
(5) keyCertSign	-	0
(6) crlSign	-	0
(7) encipherOnly	-	0
(8) decipherOnly	-	0
extendedKeyUsage 2.5.29.37	NO	1.3.6.1.5.5.7.3.1 #id-kp-serverAuth
authorityKeyIdentifier	NO	-

2.5.29.35		
keyIdentifier	-	# identifier of the CA key, for verification of the certificate signature
subjectKeyIdentifier 2.5.29.14	NO	# identifier of the certificate holder's key identified in the subjectPublicKeyInfo field
basicConstraints 2.5.29.19	NO	-
cA	-	FALSE
netscapeCertType 2.16.840.1.113730.1.1	NO	sslServer #40h
subjectAltName 2.5.29.17	NO	# alternative name of the certificate holder
rfc822Name	-	# e-mail address of the certificate holder
dNSName		# server domain name (optional field, multiple occurrence allowed)
iPAddress		# server IP address (optional field, multiple occurrence allowed)
cRLDistributionPoint 2.5.29.31	NO	-
distributionPoint	-	http://www.bptp.lodz.telekomunikacja.pl/repozytorium/crl/catp.crl
certificatePolicies 2.5.29.32	NO	-
policyIdentifier	-	1.3.6.1.4.1.27154.1.1.20.10.1.1.7
policyQualifierID 1.3.6.1.5.5.7.2.1	-	http://www.bptp.lodz.telekomunikacja.pl/repozytorium/docs/pc_bptp_1_7.pdf
qualifier 1.3.6.1.5.5.7.2.2	-	Certyfikat wystawiony zgodnie z dok. "Polityka Certyfikacji - Bezpieczna Poczta Korporacyjna Telekomunikacja Polska". Nie jest certyfikatem kwalifikowanym w rozumieniu ustawy o podpisie elektronicznym # (Certificate issued in compliance with the "Certificate Policy — Telekomunikacja Polska Secure Corporate Mail" document. Not a qualified certificate as defined by the Digital Signature Act)

For a server operated as an SSL client, the certificate has the following structure:

Attribute	Value
version	2 # certificate compliant with X.509 v. 3
serialNumber	# a number assigned by TP CA, unique within the authority
signature	1.2.840.113549.1.1.5 #SHA1 with RSA encryption (identifier of the algorithm used for electronic confirmation of the certificate)
issuer	C = PL, O = Grupa TELEKOMUNIKACJA POLSKA OU = Centrum Certyfikacji Signet, OU = CA TELEKOMUNIKACJA POLSKA # specific name of the CA issuing the certificates hereunder
validity	# certificate validity period
not before	# certificate issuance date and time (GMT in the UTCTime format)
not after	# certificate issuance date and time + 1,096 days (GMT in the UTCTime format)
subject	C = PL O = Grupa TELEKOMUNIKACJA POLSKA OU = TELEKOMUNIKACJA POLSKA OU = SSL CN = # server IP address or domain name
subjectPublicKeyInfo	
algorithm	rsaEncryption # identifier of the algorithm associated with the certificate holder's public key
subjectPublicKey	# certificate holder's public key

The certificate contains the following extensions compliant with X.509:

Extension	Critical extension?	Value
keyUsage 2.5.29.15	YES	80h
(0) digitalSignature	-	1 # digital signature key
(1) nonRepudiation	-	0
(2) keyEncipherment	-	0
(3) dataEncipherment	-	0
(4) keyAgreement	-	0
(5) keyCertSign	-	0
(6) crlSign	-	0
(7) encipherOnly	-	0
(8) decipherOnly	-	0
extendedKeyUsage 2.5.29.37	NO	1.3.6.1.5.5.7.3.2 #id-kp-clientAuth
authorityKeyIdentifier 2.5.29.35	NO	-
keyIdentifier	-	# identifier of the CA key, for verification of the certificate signature
subjectKeyIdentifier 2.5.29.14	NO	# identifier of the certificate holder's key identified in the subjectPublicKeyInfo field
basicConstraints 2.5.29.19	NO	-
cA	-	FALSE
netscapeCertType 2.16.840.1.113730.1.1	NO	sslClient #80h
subjectAltName 2.5.29.17	NO	# alternative name of the certificate holder
rfc822Name	-	# e-mail address of the certificate holder
dNSName		# server domain name (optional field, multiple occurrence allowed)
iPAddress		# server IP address (optional field, multiple occurrence allowed)
cRLDistributionPoint 2.5.29.31	NO	-
distributionPoint	-	http://www.bptp.lodz.telekomunikacja.pl/repozytorium/crl/catp.crl
certificatePolicies 2.5.29.32	NO	-
policyIdentifier	-	1.3.6.1.4.1.27154.1.1.20.10.1.1.7
policyQualifierID 1.3.6.1.5.5.7.2.1	-	http://www.bptp.lodz.telekomunikacja.pl/repozytorium/docs/pc_bptp_1_7.pdf
qualifier 1.3.6.1.5.5.7.2.2	-	Certyfikat wystawiony zgodnie z dokumentem "Polityka Certyfikacji - Bezpieczna Poczta Korporacyjna Telekomunikacja Polska". Nie jest certyfikatem do weryfikacji podpisu elektronicznego. # (Certificate issued in compliance with the "Certificate Policy — Telekomunikacja Polska Secure Corporate Mail" document. Not a certificate for verification of a digital signature.)

For a server operated as both an SSL client and SSL server, the certificate has the following structure:

Attribute	Value
version	2 # certificate compliant with X.509 v. 3
serialNumber	# a number assigned by TP CA, unique within the authority
signature	1.2.840.113549.1.1.5 #SHA1 with RSA encryption (identifier of the algorithm used for electronic confirmation of the certificate)
issuer	C = PL, O = Grupa TELEKOMUNIKACJA POLSKA

	OU = Centrum Certyfikacji Signet, OU = CA TELEKOMUNIKACJA POLSKA # specific name of the CA issuing the certificates hereunder
validity	# certificate validity period
not before	# certificate issuance date and time (GMT in the UTCTime format)
not after	# certificate issuance date and time + 1,096 days (GMT in the UTCTime format)
subject	C = PL O = Grupa TELEKOMUNIKACJA POLSKA OU = TELEKOMUNIKACJA POLSKA OU = SSL CN = # server IP address or domain name
subjectPublicKeyInfo	
algorithm	rsaEncryption # identifier of the algorithm associated with the certificate holder's public key
subjectPublicKey	# certificate holder's public key

The certificate contains the following extensions compliant with X.509:

Extension	Critical extension?	Value
keyUsage 2.5.29.15	YES	80h
(0) digitalSignature	-	1 # digital signature key
(1) nonRepudiation	-	0
(2) keyEncipherment	-	1 # key-exchange key
(3) dataEncipherment	-	1 # data encryption key
(4) keyAgreement	-	0
(5) keyCertSign	-	0
(6) crlSign	-	0
(7) encipherOnly	-	0
(8) decipherOnly	-	0
extendedKeyUsage 2.5.29.37	NO	1.3.6.1.5.5.7.3.2 #id-kp-clientAuth 1.3.6.1.5.5.7.3.1 #id-kp-serverAuth
authorityKeyIdentifier 2.5.29.35	NO	-
keyIdentifier	-	# identifier of the CA key, for verification of the certificate signature
subjectKeyIdentifier 2.5.29.14	NO	# identifier of the certificate holder's key identified in the subjectPublicKeyInfo field
basicConstraints 2.5.29.19	NO	-
cA	-	FALSE
subjectAltName 2.5.29.17	NO	# alternative name of the certificate holder
rfc822Name	-	# e-mail address of the certificate holder
dNSName		# server domain name (optional field, multiple occurrence allowed)
iPAddress		# server IP address (optional field, multiple occurrence allowed)
cRLDistributionPoint 2.5.29.31	NO	-
distributionPoint	-	http://www.bptp.lodz.telekomunikacja.pl/repozytorium/crl/catp.crl
certificatePolicies 2.5.29.32	NO	-
policyIdentifier	-	1.3.6.1.4.1.27154.1.1.20.10.1.1.7
policyQualifierID 1.3.6.1.5.5.7.2.1	-	http://www.bptp.lodz.telekomunikacja.pl/repozytorium/docs/pc_bptp_1_7.pdf
qualifier 1.3.6.1.5.5.7.2.2	-	Certyfikat wystawiony zgodnie z dokumentem "Polityka Certyfikacji - Bezpieczna Poczta Korporacyjna

		Telekomunikacja Polska". Nie jest certyfikatem do weryfikacji podpisu elektronicznego. # (Certificate issued in compliance with the "Certificate Policy — Telekomunikacja Polska Secure Corporate Mail" document. Not a certificate for verification of a digital signature.)
--	--	---

7.4 VPN certificate profile

A VPN certificate has the following structure:

Attribute	Value
version	2 # certificate compliant with X.509 v. 3
serialNumber	# a number assigned by TP CA, unique within the authority
signature	1.2.840.113549.1.1.5 #SHA1 with RSA encryption (identifier of the algorithm used for electronic confirmation of the certificate)
issuer	C = PL, O = Grupa TELEKOMUNIKACJA POLSKA OU = Centrum Certyfikacji Signet, OU = CA TELEKOMUNIKACJA POLSKA # specific name of the CA issuing the certificates hereunder
validity	# certificate validity period
not before	# certificate issuance date and time (GMT in the UTCTime format)
not after	# certificate issuance date and time + 1,096 days (GMT in the UTCTime format)
subject	C = PL O = Grupa TELEKOMUNIKACJA POLSKA OU = TELEKOMUNIKACJA POLSKA OU = VPN CN = # server IP address or domain name
subjectPublicKeyInfo	
algorithm	rsaEncryption # identifier of the algorithm associated with the certificate holder's public key
subjectPublicKey	# certificate holder's public key

The certificate contains the following extensions compliant with X.509:

Extension	Critical extension?	Value
keyUsage 2.5.29.15	YES	80h
(0) digitalSignature	-	1 # digital signature key
(1) nonRepudiation	-	0
(2) keyEncipherment	-	1 # key-exchange key
(3) dataEncipherment	-	1 # data encryption key
(4) keyAgreement	-	0
(5) keyCertSign	-	0
(6) crlSign	-	0
(7) encipherOnly	-	0
(8) decipherOnly	-	0
extendedKeyUsage 2.5.29.37	NO	1.3.6.1.5.5.8.2.2 #XCN_OID_IPSEC_KP_IKE_INTERMEDIATE (optional extension ⁽¹⁾)
authorityKeyIdentifier 2.5.29.35	NO	-
keyIdentifier	-	# identifier of the CA key, for verification of the certificate signature
subjectKeyIdentifier 2.5.29.14	NO	# identifier of the certificate holder's key identified in the subjectPublicKeyInfo field
basicConstraints 2.5.29.19	NO	-

cA	-	FALSE
subjectAltName 2.5.29.17	NO	# alternative name of the certificate holder
iPAddress		# device IP address (optional field)
dNSName		# device domain name (optional field)
rfc822Name	-	# e-mail address of the certificate holder (optional field)
cRLDistributionPoint 2.5.29.31	NO	-
distributionPoint	-	http://www.bptp.lodz.telekomunikacja.pl/repozytorium/crl/catp.crl
certificatePolicies 2.5.29.32	NO	-
policyIdentifier	-	1.3.6.1.4.1.27154.1.1.20.10.1.1.7
policyQualifierID 1.3.6.1.5.5.7.2.1	-	http://www.bptp.lodz.telekomunikacja.pl/repozytorium/docs/pc_bptp_1_7.pdf
qualifier 1.3.6.1.5.5.7.2.2	-	Certyfikat wystawiony zgodnie z dokumentem "Polityka Certyfikacji - Bezpieczna Poczta Korporacyjna Telekomunikacja Polska". Nie jest certyfikatem do weryfikacji podpisu elektronicznego. # (Certificate issued in compliance with the "Certificate Policy — Telekomunikacja Polska Secure Corporate Mail" document. Not a certificate for verification of a digital signature.)

⁽¹⁾ If provided in the certificate request or is required for technical reasons.

7.5 Domain-controller certificate profile

A domain-controller certificate has the following structure:

Attribute	Value
version	2 # certificate compliant with X.509 v. 3
serialNumber	# a number assigned by TP CA, unique within the authority
signature	1.2.840.113549.1.1.5 #SHA1 with RSA encryption (identifier of the algorithm used for electronic confirmation of the certificate)
issuer	C = PL, O = Grupa TELEKOMUNIKACJA POLSKA OU = Centrum Certyfikacji Signet, OU = CA TELEKOMUNIKACJA POLSKA # specific name of the CA issuing the certificates hereunder
validity	# certificate validity period
not before	# certificate issuance date and time (GMT in the UTCTime format)
not after	# certificate issuance date and time + 1,096 days
subject	CN = # domain name of the domain controller OU = # name of the organizational unit or device group (optional field) DC = # domain name fragments, as provided in the certificate request (multiple occurrence allowed)
subjectPublicKeyInfo	
algorithm	1.2.840.113549.1.1.1 rsaEncryption # identifier of the algorithm associated with the certificate holder's public key
subjectPublicKey	# certificate holder's public key

The certificate contains the following extensions compliant with X.509:

Extension	Critical extension?	Value
keyUsage (2.5.29.15)	YES	A0h # 'h' designates the hexadecimal notation
(0) digitalSignature	-	1 # digital signature key
(1) nonRepudiation	-	0

(2) keyEncipherment	-	1 # key-exchange key
(3) dataEncipherment	-	0
(4) keyAgreement	-	0
(5) keyCertSign	-	0
(6) crlSign	-	0
(7) encipherOnly	-	0
(8) decipherOnly	-	0
extendedKeyUsage 2.5.29.37	NO	1.3.6.1.5.5.7.3.2 #id-kp-clientAuth 1.3.6.1.5.5.7.3.1 # id-kp-serverAuth
certificateTemplateName 1.3.6.1.4.1.311.20.2	NO	DomainController
authorityKeyIdentifier 2.5.29.35	NO	-
keyIdentifier	-	# identifier of the CA key, for verification of the certificate signature
subjectKeyIdentifier 2.5.29.14	NO	# identifier of the certificate holder's key identified in the subjectPublicKeyInfo field
basicConstraints 2.5.29.19	NO	-
cA	-	FALSE
subjectAltName 2.5.29.17	NO	# alternative name of the certificate holder
otherName		1.3.6.1.4.1.311.25.1 = # GUID value as provided in the certificate request (Note: only capital letters are allowed)
dNSName		# server domain name as provided in the certificate request
rfc822Name	-	# e-mail address of the Administrator (certificate holder)
cRLDistributionPoint 2.5.29.31	NO	-
distributionPoint	-	http://www.bptp.lodz.telekomunikacja.pl/repozytorium/crl/catp.crl
certificatePolicies 2.5.29.32	NO	-
policyIdentifier	-	1.3.6.1.4.1.27154.1.1.20.10.1.1.7
policyQualifierID 1.3.6.1.5.5.7.2.1	-	http://www.bptp.lodz.telekomunikacja.pl/repozytorium/docs/pc_bptp_1_7.pdf
qualifier 1.3.6.1.5.5.7.2.2	-	Certyfikat wystawiony zgodnie z dokumentem "Polityka Certyfikacji - Bezpieczna Poczta Korporacyjna Telekomunikacja Polska". Nie jest certyfikatem do weryfikacji podpisu elektronicznego. # (Certificate issued in compliance with the "Certificate Policy — Telekomunikacja Polska Secure Corporate Mail" document. Not a certificate for verification of a digital signature.)

7.6 Software certificate profile

A software certificate has the following structure:

Attribute	Value
version	2 # certificate compliant with X.509 v. 3
serialNumber	# a number assigned by TP CA, unique within the authority
signature	1.2.840.113549.1.1.5 #SHA1 with RSA encryption (identifier of the algorithm used for electronic confirmation of the certificate)
issuer	C = PL, O = Grupa TELEKOMUNIKACJA POLSKA OU = Centrum Certyfikacji Signet, OU = CA TELEKOMUNIKACJA POLSKA # specific name of the CA issuing the certificates hereunder
validity	# certificate validity period
not before	# certificate issuance date and time (GMT in the UTCTime format)

not after	# certificate issuance date and time + 1,096 days (GMT in the UTCTime format)
subject	C = PL, O = Grupa TELEKOMUNIKACJA POLSKA, OU = # TELEKOMUNIKACJA POLSKA CN = # as provided in the certificate request givenName= # given name of the certificate holder (optional attribute) surName= # surname of the certificate holder (optional attribute)
subjectPublicKeyInfo	
algorithm	1.2.840.113549.1.1.1 # rsaEncryption — identifier of the algorithm associated with the certificate holder's public key
subjectPublicKey	# certificate holder's public key

The certificate contains the following extensions compliant with X.509:

Extension	Critical extension?	Value
keyUsage 2.5.29.15	YES	80h
(0) digitalSignature	-	1 # digital signature key
(1) nonRepudiation	-	0
(2) keyEncipherment	-	0
(3) dataEncipherment	-	0
(4) keyAgreement	-	0
(5) keyCertSign	-	0
(6) crlSign	-	0
(7) encipherOnly	-	0
(8) decipherOnly	-	0
extendedKeyUsage 2.5.29.37	NO	1.3.6.1.5.5.7.3.3 #id-kp-codeSigning
authorityKeyIdentifier 2.5.29.35	NO	-
keyIdentifier	-	# identifier of the CA key, for verification of the certificate signature
subjectKeyIdentifier 2.5.29.14	NO	# identifier of the certificate holder's key identified in the subjectPublicKeyInfo field
basicConstraints 2.5.29.19	NO	-
cA	-	FALSE
netscapeCertType 2.16.840.1.113730.1.1	NO	objectSigning #10h ('h' designates the hexadecimal notation)
subjectAltName 2.5.29.17	NO	# alternative name of the certificate holder
rfc822Name	-	# e-mail address of the person responsible for using the certificate
cRLDistributionPoint 2.5.29.31	NO	-
distributionPoint	-	http://www.bptp.lodz.telekomunikacja.pl/repozytorium/crl/catp.crl
certificatePolicies 2.5.29.32	NO	-
policyIdentifier	-	1.3.6.1.4.1.27154.1.1.20.10.1.1.7
policyQualifierID 1.3.6.1.5.5.7.2.1	-	http://www.bptp.lodz.telekomunikacja.pl/repozytorium/docs/pc_bptp_1_7.pdf
qualifier 1.3.6.1.5.5.7.2.2	-	Certyfikat wystawiony zgodnie z dokumentem "Polityka Certyfikacji - Bezpieczna Poczta Korporacyjna Telekomunikacja Polska". Nie jest certyfikatem kwalifikowanym w rozumieniu Ustawy. (Certificate issued in

		compliance with the “Certificate Policy — Telekomunikacja Polska Secure Corporate Mail” document. Not a qualified certificate as defined by the Digital Signature Act)
--	--	--

7.7 Test certificate profiles

Test profiles issued hereunder have exactly the same profiles as the corresponding regular profiles, except for the validity period which may not exceed 60 days.

validity	# certificate validity period
not before	# certificate issuance date and time (GMT in the UTCTime format)
not after	# certificate issuance date and time + not more than 60 days

7.8 Certificate Revocation List (CRL) profile

A CRL has the following structure:

Attribute	Value
version	1 # list compliant with X.509 v. 2
signature	1.2.840.113549.1.1.5 #SHA1 with RSA encryption (identifier of the algorithm used for signing the CRL)
issuer	C = PL, O = Grupa TELEKOMUNIKACJA POLSKA OU = Centrum Certyfikacji Signet, OU = CA TELEKOMUNIKACJA POLSKA # specific name of the CA issuing the certificates hereunder
thisUpdate	# list publication date and time (GMT in the UTCTime format)
nextUpdate	# list publication date + not more than 72 hours (GMT in the UTCTime format)
revokedCertificates	# list of revoked certificates, with the following syntax:
serialNumber	# serial number of the revoked certificate
revocationDate	# revocation date
reasonCode 2.5.29.21	# revocation reason

The **reasonCode** field is a non-critical extension of the **revokedCertificates** field, specifying the reason of revocation or indicating that the certificate is suspended. The allowed values are as follows:

- unspecified (0)
- keyCompromise (1) — the key has been compromised
- cACompromise (2) — the CA key has been compromised
- affiliationChanged (3) — the certificate holder data has been changed
- superseded (4) — the key has been superseded (renewed)
- cessationOfOperation (5) — the certificate ceased to be used for its purpose
- certificateHold (6) — the certificate has been suspended.

The CRL contains the following extensions:

Extension	Critical extension?	Value
cRLNumber 2.5.29.20	NO	# CRL number assigned by TP CA
authorityKeyIdentifier 2.5.29.35	NO	
keyIdentifier	-	# identifier of the CA key, for electronic verification of the CRL